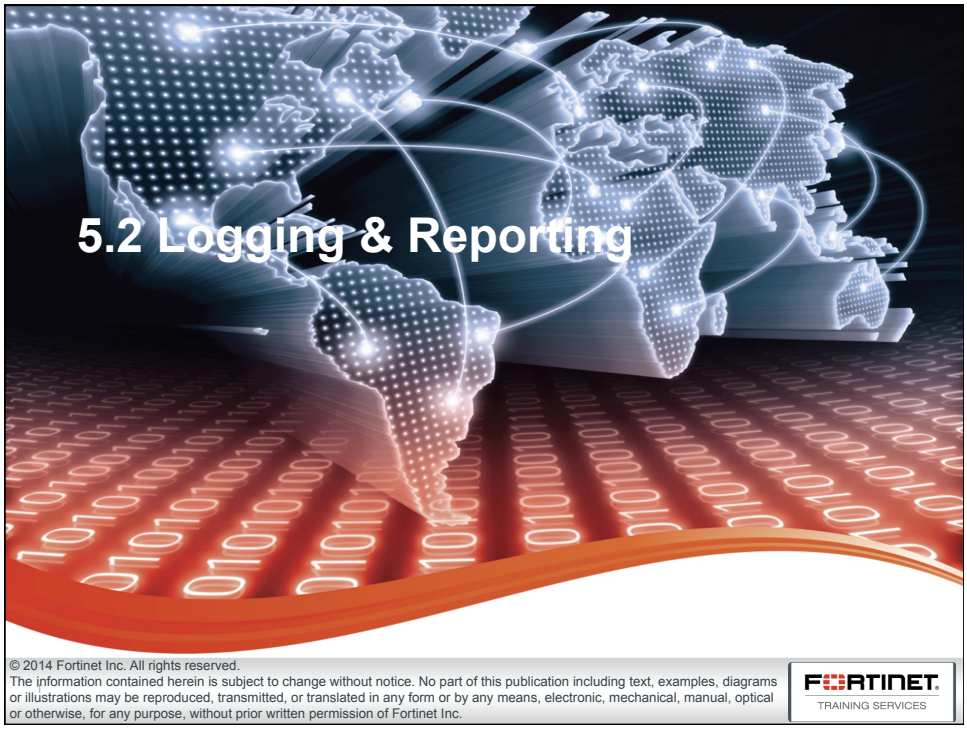


FORTINET TRAINING SERVICES

Logging & Reporting: New Features & Changes

- Sniffer Log
- Report log Source
- Process Crash behavior
- 5 point rating for “Application Risk”

FORTINET

Sniffer Log

- When an interface is operating in One-Arm sniffer mode the traffic log will go to Log & Report > Traffic Log > Sniffer Log
  - » Previously logs were sent to Forward traffic, impossible to tell which logs were normal which were sniffer based (if the device was doing both).
  - » extended-utm-log enabled profiles still create logs in Security Log section

3 FORTINET

Report log source

- Reports can look at the Forward traffic log, Sniffer log or both

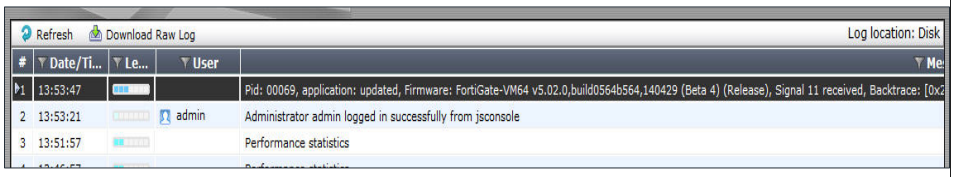
```
config report setting
        set status enable
        set report-source {forward-traffic|sniffer-traffic|both}
end
```

- Allows report output to be separated from traffic passing though the device and traffic being inspected using One-Arm mode.

4 FORTINET

Process crash behavior

- Processes crashes will show in the event log in an abbreviated format.
  - » Anytime a process shuts down it's a "Crash"
  - » Some "Crashes" are intentional
    - EG: Scanunit shuts down (crashes) to update AV database
    - Reason for "Crash" is based on the Signal number (Unix OS)



5

5 Point "Application Risk" rating

Icon	Risk Level	Description	Example
	Critical	Applications that are used to conceal activity to evade detection	Tor, SpyBoss
	High	Applications that can cause data leakage, or prone to vulnerabilities or downloading malware	Remote Desktop, File Sharing, P2P
	Medium	Applications that can be misused	VoiP, Instant Messaging, File Storage, WebEx, Gmail
	Elevated	Applications are used for personal communications or can lower productivity	Gaming, Facebook, Youtube
	Low	Business Related Applications or other harmless applications	Windows Updates

6

FORTINET TRAINING SERVICES

UTM: New Features & Changes

- SSL
- Antivirus
- Web Filtering
- App Control
- DoS
- IPS

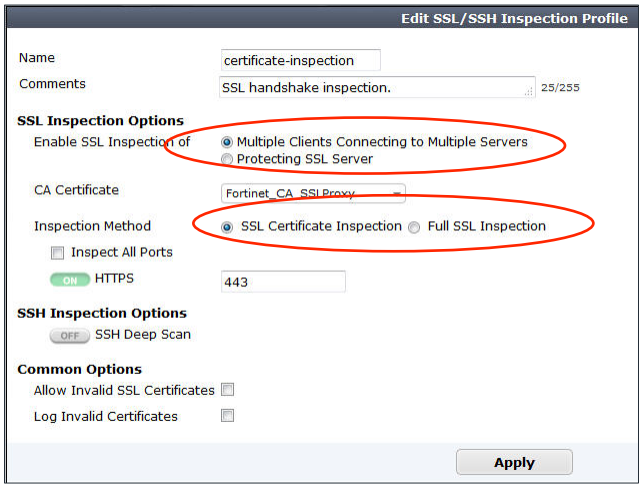
FORTINET

SSL

- Overall configuration simplification for how encrypted traffic is handled
  - » No secure protocol options in any other security profile
  - » How Encrypted traffic is handled is based entirely on setting SSL/ SSH profile
- Enabling an SSL/SSH profile is REQUIRED when enabling ANY other UTM profile
  - » 5.0.x (and earlier) SSL/SSH profile was used ONLY TO ENABLE SSL Deep scanning
  - » 5.2 SSL/SSH Profile is used to determine ***how*** encrypted traffic should be handled
    - Man-in-the-Middle content scanning vs Certificate scan

9

SSL: SSL/SSH Profile



10

Antivirus: Traditional Flow based inspection AV Limits

- Flow based inspection can not handle any action that needs to full file to perform
  - » Scanning inside archives
  - » Identifying some viruses & variants
  - » Identifying viruses that hide in multiple portions of the file
    - Files are scanned through small windows
    - Windows are stateless (results from 1 window are not related to any other)
- Replacement Messages
  - » Depending on where detection happens within file transmission a replacement message may not be possible until client refreshes/ restarts connection.
- Summary: Lower Accuracy

11 FORTINET

Antivirus: Flow based inspection AV Advantages

- Transmission Speed
  - » Traffic is not cached, and scanned before sending
- No Modification of packets
  - » A proxy breaks layer 3 communication
- File Size is not a limiting factor
  - » Traffic scanned continuously as a stream
  - » Scanning is not done on entire file, at once
- Summary: Higher throughput

12 FORTINET

Antivirus: Flow based AV Scanning improvement

- Flow based AV now behaves similar to Proxy AV
  - » Traffic is cached in memory, but not proxyed
    - Layer 2 communication unbroken
  - » Scanning is done on the entire file, rather then a small window
    - Max File size effects Proxy/Flow AV the same
    - Scanning within archives is possible

"IPS will accumulate data until it detect the end of file. Then it'll pause the traffic and asynchronously send data to the scanunitd for analysis. Upon receiving result it will either unpause the traffic or reset the connection."

- » Only 1 AV database is needed
  - scanunitd is the Proxy AV scanner
  - Saves memory space due to removal of separate Flow AV database.

13 FORTINET

Antivirus: Default AV setting

- Default AV profile uses Flow AV, not proxy
  - » Proxy & Flow based UTM inspection can't be combined in a single policy.
- New AV profiles will also use Flow AV, by default

14 FORTINET

Web filtering: Change Recap

- All HTTPS related options moved out of WF Profile to SSL profile
  - SSL exemption by category
- Support for SNI inspection (added in a 5.0.x patch)
  - CA inspection is weak
  - Modern browsers transmit URL details plain text when accessing HTTPS
  - Allows for complete URL inspection without being part of SSL communication
  - AV & other content inspection needs MITM

15

Web filtering: More detail on Flow based block pages

- Additional details have been added to the Flow based block pages.
  - Web Site
  - Category
  - Username
  - IP
  - Etc..

16

Web filtering: Force HTTPS Warn & Authentication pages

- When the FortiGuard Website action is Authentication or the user does an Override (if enabled) HTTPS can be forced
  - » Previously the page used the same protocol the website being requested

```
config webfilter fortiguard
  set ovrd-auth-https {disable | enable} (WF Authentication page)
  set warn-auth-https {disable | enable} (WF Warning page)
end
```

17 FORTINET

Web filtering: Add “Referrer” field to URL filter list

- URL Filter list has added support to specify a Referrer field as part of an entry
  - » CLI only unless `gui-webfilter-advanced` is enabled under `config sys global`
- Allows websites to be blocked/allowed except when clicking a link on another website

Enable URL Filter

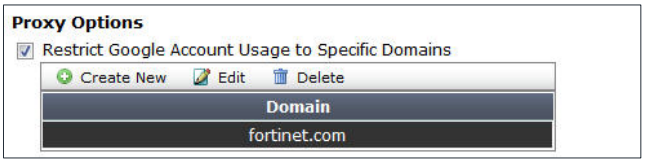
Create New | Edit | Delete

URL	Type	Action	Status	Referrer
.facebook.	Wildcard	Monitor	Enable	MyFortinet.com
.facebook.	Wildcard	Block	Enable	

18 FORTINET

Web filtering: Restricting Google access

- Restrict login to google to only allow specific domains
  - » Proxy WF only
  - » Allows a workplace to restrict google access to only their corporate accounts.



19

Web filtering: SSL Certificate replacement

- Support added for SSL Certificate replacement when using Certificate inspection mode
  - » In order to avoid HTTPS warning messages when SSL Deep Scanning is NOT USED and the FortiGate generates a block age the FortiGate will generate a block page using the CA for the current SSL session
  - » MAY NOT match the website. Sometimes SSL is re-encrypted after the first establishment, which may use other certificates that can't be seen without Man-in-the-middle inspection.
    - If multiple SSL re-encyption handshakes are done, only the CA from the first certificate can be pulled out. Will still avoid browser warning messages.

20

Application Control: Inline SSL decoding

- **Only works if deep scanning is enabled and all UTM features are flow-based modes.**
  - » Inline mode kicks in automatically, no configuration is needed
- IPS engine is used for scanning the traffic.
- No session termination is performed
  - » Does not break layer 3 communications (like SSL Proxy)
- FGT modifies the key negotiation to decrypt as needed

21

Application Control: What SSL can be Decoded inline?

- Technologies supported with this change:

Client Channel

Next Protocol Negotiation (NPN)

App-Layer Protocol Negotiation (ALPN)

SPDY 2/3.0/3.1 versions

- FortiOS 5.0 could not make use of SPDY when doing deep inspection, proxy would force plain HTTP instead
- 5.2 can support SPDY with inline SSL inspection. MITM is performed in a different way.

22

Inline SSL Decoding: What is Next Protocol Negotiation?

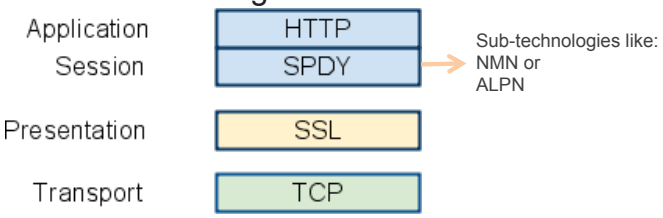
- Chrome TLS extension to control app-layer protocol negotiation
- Helps choose which protocols should be used over a secure connection to avoid unnecessary round trips
- Is being phased out. Disabled in Chrome 20 and higher (unless website with the NPN extension)
- Will be replaced with ALPN

Inline SSL Decoding: Application Layer Protocol Negotiation

- TLS extension that facilitates the agreement between two peers on which custom protocol will be used during an HTTPS session up-front
- Can be seen in packet captures in the 'ProtocolNameList' (ClientHello) and 'ProtocolName' (ServerHello) fields
- Client specifies the protocols supported, server confirms (opposite of NPN)
- Protocols listed in the exchange use IANA's numbering

Inline SSL Decoding: Speedy (SPDY)

- App layer protocol designed for minimal latency
- Adds a session layer over SSL for multiple concurrent, interleaved streams over a single TCP connection.



- Pioneered by Google
- Selected as the 'base' protocol for HTTP v2, currently augments HTTP 1

25

Inline SSL Decoding with SPDY: How useful is it?

- Supported in Chrome (all), Firefox (2-3.1), Opera and IE (IE11 supports v3)
- About .6% of web servers support it. Facebook and Twitter are popular examples
- Will be switching from NPM to ALPN soon
- Has no support for port 80, all communication is secured over 443 via TLS
- **Starting in FortiOS 5.2 deep inspection clients will be able to take advantage of SPDY as long as they are using flow-based UTM**

26

Application Control: Additional Cloud based information

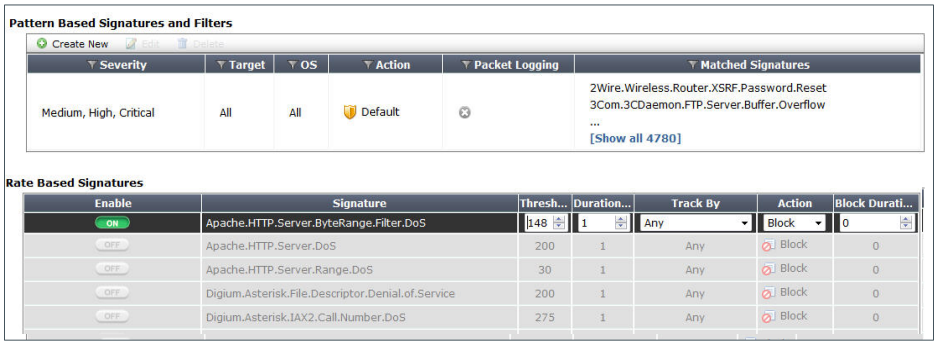
- Information about user logins and file transfers for cloud applications.
- Video names for many popular video streaming including YouTube, NetFlix, Vevo, Dailymotion, Veoh, Hulu, Vube, Metacafe, LiveLeak, Break, and Ustream.
  - clouduser, cloudaction, filename, and filesize added to traffic and App Control logs

DoS: IPv6 Acceleration

- XLP processors can now accelerate IPv6 DoS policys
  - Generally only effects larger device (FG 5101C)
  - Could result in significant CPU reduction (depending on traffic and configuration)

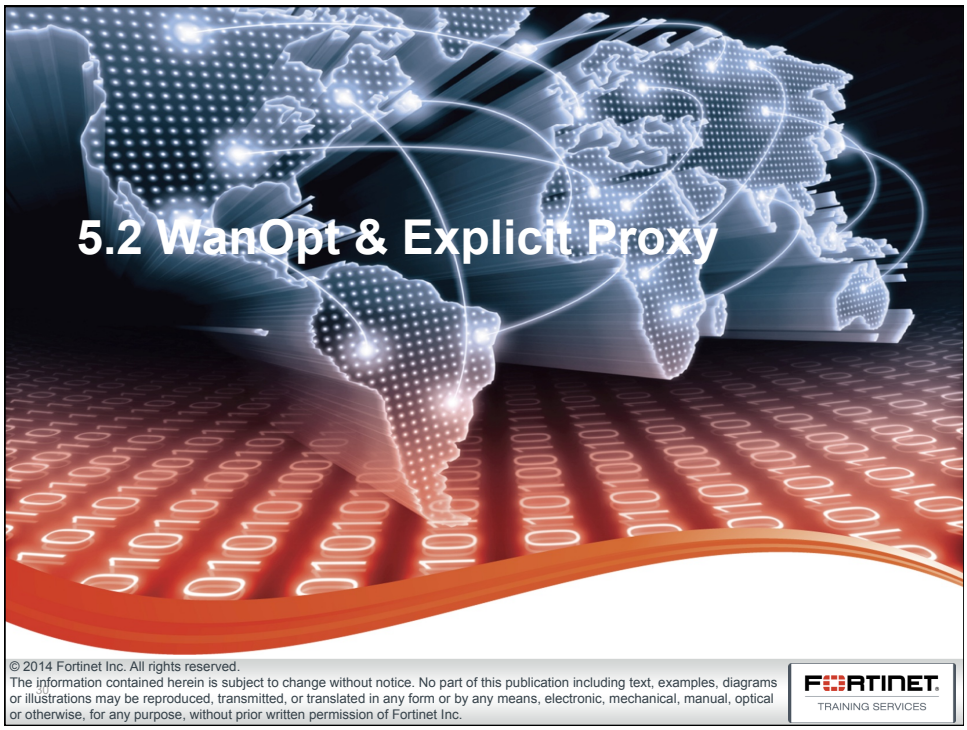
IPS: Rate based detection from the GUI

- Some IPS signature can be configure to operate based on the rate of detection (vs single incident)
  - » Custom signature syntax for rate as well
  - » Support added 5.0.x (CLI)



29

FORTINET



FORTINET
TRAINING SERVICES

Wanopt & Explicit proxy: New Features & Changes

- Performance improvement
- Policy Configuration Change
- IP Reflect
- URL Address object type
- Add/Remove HTTP headers

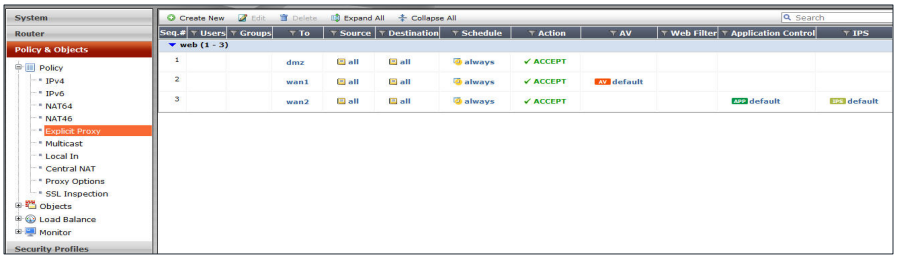
Performance Improvement

- Multiple instances of or Web proxy daemon on devices with multiple CPU cores
  - » Default 1
  - » Useful on larger devices that make heavy use of the explicit proxy

```
config system global
      set wad-worker-count <1 – CPU>
end
```

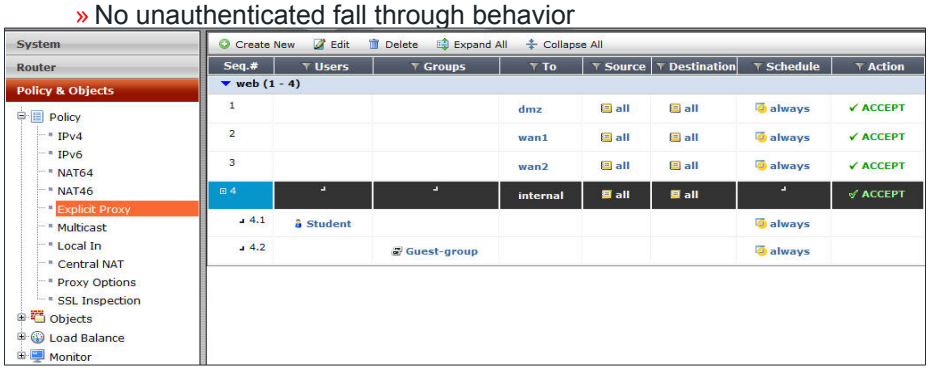
Policy Configuration Change: New Section

- Previously Explicit proxy policies were setup in the same section as Firewall policies
  - » New Policy section for explicit proxy
  - » Destination interface is specified
  - » Source is any/all interfaces listening for explicit proxy connections
  - » GUI Controls are not the same as for firewall policys



Policy Configuration Change: Authentication

- Authentication handled through “Authenticate” action on policy
  - » Sub-rules within policy define allowed use action(s)
  - » No unauthenticated fall through behavior



Policy Configuration Change: SSO_guest_user group

- 2 types of authentication
  - Passive (no user prompt), FSSO, etc.
  - Active (user prompted), Local, LDAP, etc.
- 4 possible situations for authentication
  - 1. User is not authenticated, i.e., the username has not been identified.
  - 2. User is authenticated, but not authorized by a group in the policy (passive authentication)
  - 3. User is authenticated, but not authorized by a group in the policy (active authentication)
  - 4. User is authenticated and allowed by group

35

Policy Configuration Change: Situation 1

- User is not authenticated, i.e. the username has not been identified.
- If passive authentication is used determine user (through passive method) and then, move on to situation 2
- If active authentication is used determine user (through active method) and then, move on to situation 3
- If both passive and active authentication have been enabled, passive authentication is processed first

36

Policy Configuration Change: Situation 2

- User is authenticated, but not authorized by a group in the policy (passive authentication)
- If passive authentication is used and name is not learned, use active method if configured (situation 3).
- If authentication is purely passive and username is not learned, username will become "anonymous“ and can be authorized by using the SSO_guest_user group, since there is no way to prompt a user authentication.
- Users that don’t fall into other groups within the policy can be considered part of the SSO_guest_user group, based on `strict-guest` setting

37 FORTINET

Policy Configuration Change: Situation 3

- User is authenticated, but not authorized by a group in the policy (active authentication)
- Active authentication poles user for authentication until successful
- Users that don’t fall into other groups within the policy can be considered part of the SSO_guest_user group, based on `strict-guest` setting

38 FORTINET

Policy Configuration Change: `strict-guest`

- Users that are learned (passively or actively) that are not part of a group defined in the policy can be considered part of SSO_guest_user based on strict-guest setting
  - » enabled: users must explicitly added through the CLI
  - » disabled: adding users is not required

```
config web-proxy explicit
       set strict-guest {enable|disble} : default enable
end
```

39 FORTINET

IP Reflect: Transparent Explicit Proxy

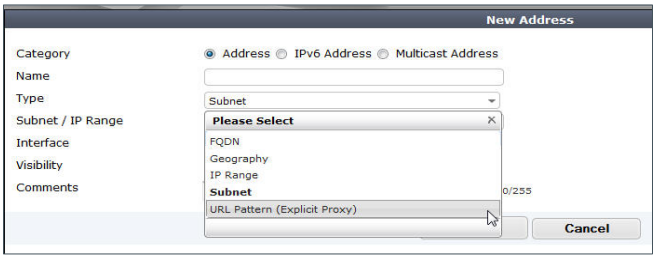
- Some software does not play well with an explicit proxy
  - » Example: Windows Update
  - » Proxy Auto Config files not always possible
    - Example: Windows Update software uses internet settings options from control panel but can't accept a PAC file
- Create Explicit proxy policy for destination and enable transparent operation
  - » Outgoing request does not alter source IP or packets
  - » Enable transparent operation in the policy via the CLI

```
config firewall explicit-proxy-policy
     edit (policy id)
     set transparent [enable|disable]
end
```

40 FORTINET

URL Address object type

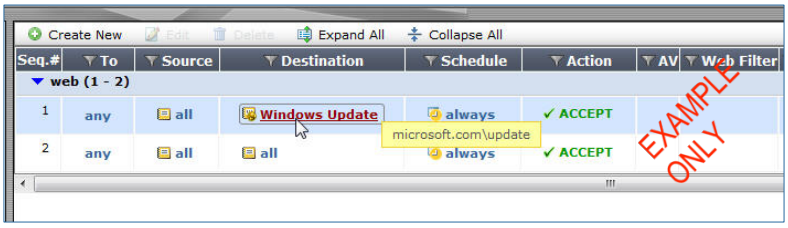
- Only for Explicit proxy
  - » Explicit proxy intercepts GET requests by design, Firewall policies do not (IP & port only)
  - » Works extremely well with “transparent” explicit proxy feature



41

Transparent and URL Address object Use Case

- Issue: Windows update through the Explicit proxy fails
  - » Make URL Address object(s) to apply to windows updates
  - » Make policy(s) using addresses as destination
  - » Set policy(s) to transparent in CLI



- THIS SOLUTION IS NOT VALID!!!!!

42

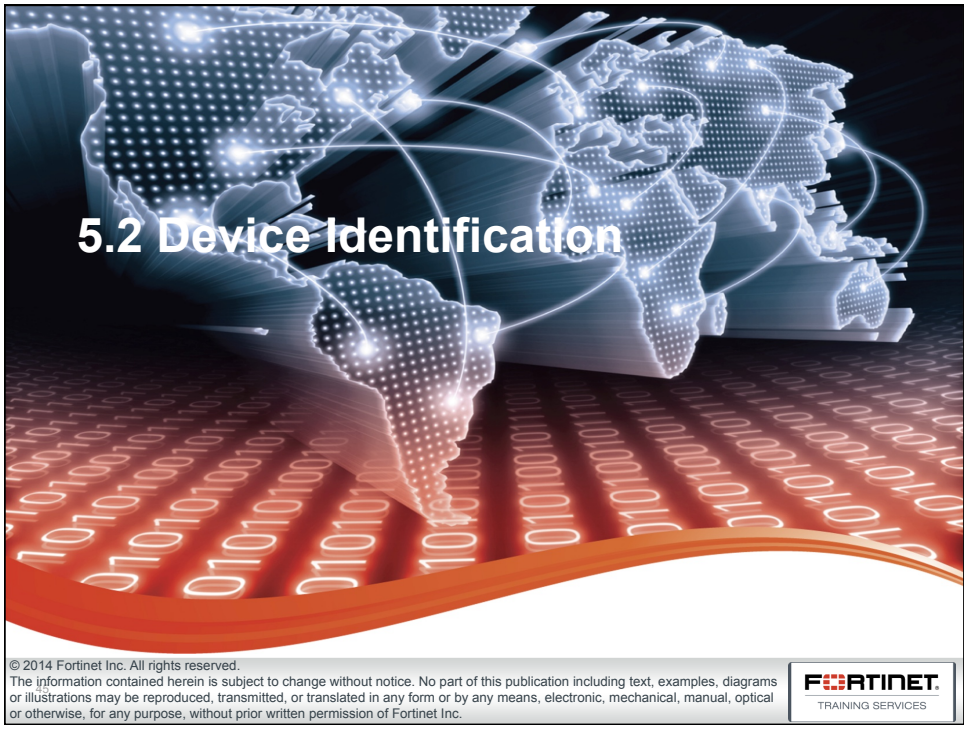
Add/Remove HTTP headers

- Previously HTTP headers could be added through explicit proxy
  - » Sometimes required for proxy chaining
- CLI edit of the profile allows for adding or removing headers
  - » Helps hide internal details when FGT is last proxy in chain to Internet

Add/Remove HTTP headers

```
config web-proxy profile
   edit (profile)
   set header-client-ip [pass | add | remove]
          set header-via-request [pass | add | remove]
          set header-via-response [pass | add | remove]
          set header-x-forwarded-for [pass | add | remove]
          set header-front-end-https [pass | add | remove]
          config headers
             edit (id)
             set name (HTTP header)
             set action [add-to-request|add-to-response|remove-from-request|remove-from-
response]
             set content (Header content, if any)
             next

end
```



FORTINET TRAINING SERVICES

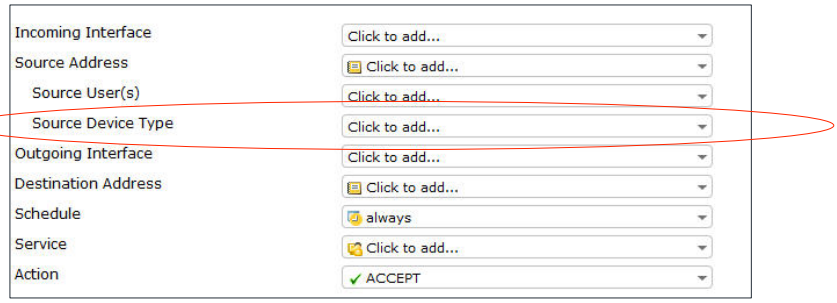
Device Identification: New Features & Changes

- New Configuration option
- New detection capabilities

FORTINET

Configuration Method

- Inside the firewall policy
  - » Can be combined with authentication



47

Detection Capabilities

- "Extended device visibility to detect devices based on traffic that does not flow through the FortiGate but which the FortiGate does see"
- Device identification is now supported for Broadcast traffic as well as traffic hitting an interface that is in One-arm sniffer mode

48

FORTINET TRAINING SERVICES

Endpoint Control

- Licensing Change

FORTINET

Licensing Change

- 5.0 Forticlient (FCT) licenses will not be supported
- 5.2 FCT licenses are yearly

- Older versions of 5.0 are still supported but with limits
  - The On-net/Off-net feature will not be supported.
  - Logging options will only appear in the CLI.
  - FortiAnalyzer Support for logging and reporting will be limited.
  - You will not be able to enter any v5.0 license keys.

End